

COURSE 9, TUTORIAL 2

WHAT ARE SBIR DATA RIGHTS AND WHY ARE THEY IMPORTANT?



SBIR/STTR Data protection is one of the most unique and important protections accorded Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) firms. These protections apply to all phases of the SBIR and STTR programs. Please note that throughout the balance of this discussion I may sometimes reference only SBIR, but that is for convenience only. Everything that I mention applies equally to the STTR program as well. One of the most important of these protections is that the government cannot disclose SBIR Data outside of the government.

The government receives a limited nonexclusive license, or right to use, SBIR/STTR Data, but such use cannot include disclosing it in any way. This nondisclosure obligation is accompanied by a protection period—four years from the end of the SBIR award for civilian awards and five years from the end of the project for military SBIR awards. A “rollover” provision contained in the SBA SBIR and STTR Directives extends these protection periods to four additional years after the end of the latest SBIR civilian award, or five years after the end of the latest military project. This places special emphasis on Phase I and II winners obtaining subsequent Phase III awards, which among other things extend the protection period for SBIR/STTR Data generated in prior Phase I, Phase II, or Phase III awards. Keep in mind that a Phase III award is by definition not paid for with Phase I or II SBIR/STTR funding. To get the most out of your participation, it is important that you prepare before the event and follow-up afterwards.

First and foremost, this nondisclosure obligation means that the government cannot compete technologies containing SBIR Data. Any such competition would mean disclosing the SBIR Data in solicitations, which the government cannot do. This unique right also underlies and supports the sole source Phase III mandate – the requirement to award Phase III awards to the SBIR developing firm *to the greatest extent practicable*. This single right – and obligation of the government – creates value in the SBIR firm and ultimately wealth for the SBIR owners.

Because of the importance of SBIR/STTR Data in the program, it is vital for small businesses to understand the nature of SBIR Data and how to protect it. It is important to understand what SBIR Data is, as well as what it is not – so that SBIR owners and their employees can better protect their technologies and SBIR Data. As we go through this analysis, one can quickly see that the SBA Directives treat SBIR and STTR Data alike.

THE IMPORTANCE OF NONDISCLOSURE

These SBIR/STTR Data protections have many implications.

WHAT IS SBIR/STTR DATA?

SBIR/STTR Data has three basic attributes: 1) it is recorded



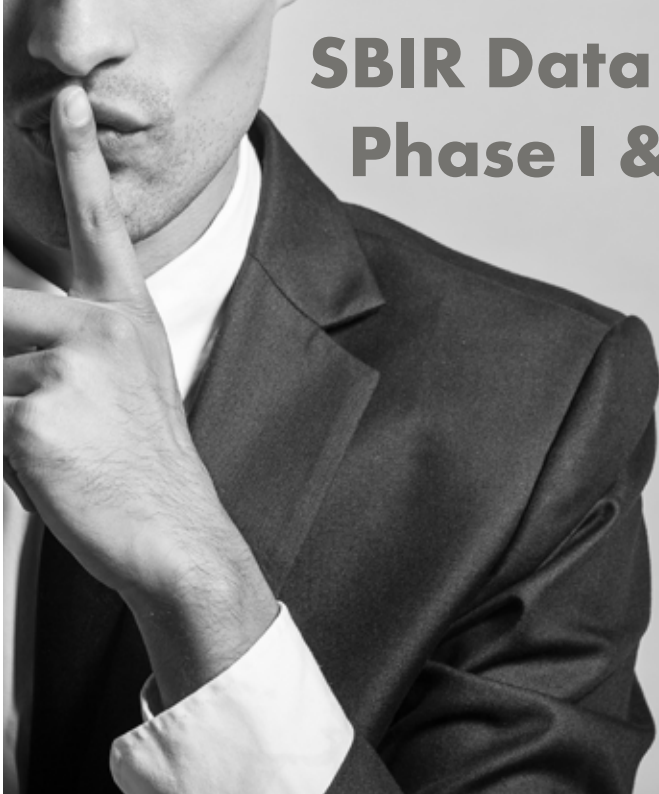
information, 2) of a technical nature, 3) that is generated under an SBIR or STTR funding agreement. We use the term “funding agreement” because SBIR awards can be grants, contracts, cooperative agreements, or any other type of funding award the government chooses to make.

SBIR/STTR data have 3 essential attributes

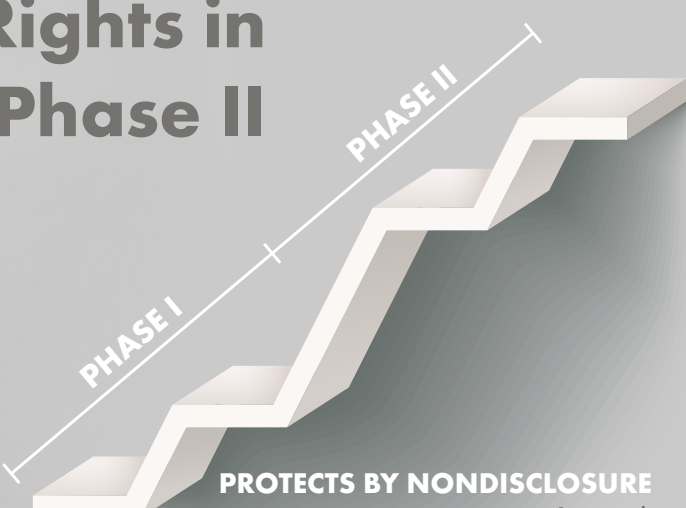
- (1) It is recorded information**
- (2) It is technical in nature**
- (3) It is generated under an SBIR or STTR funding agreement**

ware and source code through this nondisclosure obligation, because they do not wish to disclose their software architecture or actual source code in a patent.

SBIR/STTR Data must be technical in nature. Non-technical data does not qualify as SBIR Data. Cost and pricing information is a good example of this. This data is protected by the Freedom of Information Act, paragraph (b)(4), which constitutes an exception to mandatory disclosure of information by the government. It also can be subject to and protected by the Privacy Act. But the SBIR nondisclosure obligation of the government does not extend to such information. Such proprietary data is protected by these other means. Other non-



SBIR Data Rights in Phase I & Phase II



**PROTECTS BY NONDISCLOSURE
FUNDED WITH | SBIR/STTR \$
ACCORDED | SBIR Data right clause
COMMERCIAL | FAR 52.227-20
4 yrs. nondisclosure
DEFENSE | DFARS 252.227-7018
5 yrs. nondisclosure**

Let's take a look at these three attributes one at a time. First, SBIR/STTR Data must be recorded information. That is, SBIR Data must be reduced to writing and contained in a written document. SBIR Data can be source code, sketches, drawings, formulas, equations, reports, descriptions of SBIR technologies, SBIR final reports, and any other type of writing that meets all three of these criteria. SBIR Data protections, however, do not apply to ideas or concepts, unless they are reduced to writing. SBIR Data protections protect the ideas contained in a written document, but not the idea itself without the writing. In order to protect an idea or concept outside of the written description of it one must resort to patent protection. Thus, the nondisclosure protection does not protect ideas or concepts by themselves. In general, most SBIR/STTR firms protect soft-

technical information, such as background data on the company, is also not protected, and should be disclosed carefully and with that knowledge in mind. The test for this “technical” requirement is that it must relate somehow to the SBIR technology being developed in Phases I, II, and III. Therefore, this SBIR Data will be something that the SBIR firm will seek to protect. Information or data that the SBIR firm advertises on its web site is not something it feels it must protect. This could include general descriptions of its SBIR technologies that do not give up trade secret information about the technology.

Third, SBIR/STTR Data must be generated under an SBIR/STTR funding agreement. Proprietary data that the firm developed with its own private funds is not SBIR Data. It was

not developed under an SBIR award. It is protected by other means, as described above. Proposal information is also not SBIR Data, although the proposal may contain SBIR Data that was generated under prior SBIR funding agreements and is protected under them. Different laws and regulations protect proposal information and prevent its disclosure. Additionally, if SBIR Data is mixed so thoroughly with non-SBIR Data that the two types of data cannot be pulled apart, or severed from each other, then the whole body of data, including the non-SBIR Data, becomes subject to the government's non-disclosure obligation. This occurs often with respect to source code and computer software.

“Non-technical data does not qualify as SBIR/STTR data”

sions is the marking that the clauses prescribe for protecting SBIR/STTR Data. Marking SBIR/STTR Data with the proper SBIR/STTR legend is critical to protecting SBIR/STTR Data.

Marking SBIR Data with precisely the wording set forth in the two clauses, that is civilian and military is equally critical. Placing these legends on SBIR Data provides notice to federal employees handling such data that they cannot disclose it. Failure to mark data properly can lead to disclosure by the government of SBIR/STTR Data. The exact legend provided in

each clause – and they are different – should be included on the title page or front page of the SBIR document or deliverable. At the bottom of each subsequent page, state:

DIFFERENCES BETWEEN CIVILIAN AND MILITARY CLAUSES

The civilian and military versions of the SBIR/STTR clauses differ. The civilian SBIR clause is set out in the Federal Acquisition Regulation (FAR) clause 52.227-20. The defense version is located in the DFARS at 252.227-7018. These clauses are very different. The civilian version provides four years of protection – the military version five years. The civilian protection period

“This page is protected by and subject to the SBIR Data Rights clause set forth on the title page.”

The clauses differ in prescribing these markings. The defense clause requests that the expiration period date be included in a header portion of the clause. When affixing this date,

IMPORTANT SBIR/STTR CLAUSES



DFARS clause 252.227-7018 for defense

starts at the end of the civilian funding agreement. The military protection period starts at the “end of the project.” The military insisted on this distinction because of the long time it takes to close out many military contracts. Another difference is the way these clauses proprietary data, that is, data generated by the SBIR firm outside of SBIR funding agreements. The defense clause requires that such data be marked “Proprietary.” The civilian clause discourages submitting such data in the first place.

Another major difference between the civilian and military ver-



FAR clause 52.227-20 for civilian agencies

be sure to add a comma after it, and the words: “subject to section 8 of the SBA SBIR Policy Directive.” (Or STTR Directive, as the case may be.) This triggers the roll-over provision of the two Directives. The civilian clause contains no such requirement to state the end date of the protection period in the SBIR/STTR markings.

THE IMPORTANCE OF MARKING DATA

Marking SBIR/STTR Data is critical to protecting it. Because the government cannot disclose SBIR or STTR Data, an SBIR firm's

competitors can obtain such data only if they purchase the technology or acquire the SBIR firm. Be very careful not to disclose your SBIR Data voluntarily. If you make a Power Point presentation to the government, mark it with the SBIR Data Rights legend. Make certain that everyone in the room is with the government when you make the presentation. When in doubt, protect your data by marking it. When larger firms seek access to SBIR technologies, they many times pay premiums in the marketplace solely to obtain access to these SBIR technologies. Marking and preserving SBIR Data is the first step in creating such a premium value in the SBIR firm and its SBIR technologies.

POWERPOINT PRESENTATIONS

It is important in protecting SBIR Data to know what it is and what it is not. The caution not to disclose SBIR Data in PowerPoint presentations does not mean that a firm cannot make PowerPoint presentations at all, or discuss an SBIR/STTR funded technology publicly. Far from it. Rather, firms must be careful about the level of technical detail they put into such presentations, especially if they are made publicly. Statements about the capabilities of the technology, when fully developed, are certainly acceptable. Comparisons to other existing technologies are acceptable. Disclosure of test results, especially if favorable, are acceptable and should even be encouraged. However, disclosing the specifics of sketches, drawings, equations, source code and code structure, final reports, how the technology works at the technical level, and so forth would constitute a voluntary disclosure of SBIR Data and should be avoided. It is the “technical” aspect of the definition discussed above that renders SBIR Data trade secrets that must be protected. When in doubt, the rule for owners and staff should be: “Don’t disclose.”

We hope this information on SBIR and STTR Data was helpful.